

What is claimed is:

- 1 1. A method, comprising:
 - 2 parsing a data stream to find a predefined synchronization point within
 - 3 the data stream; and
 - 4 placing non-compliant data near the synchronization point in the data
 - 5 stream;
 - 6 wherein the data stream is decodable by a compliant decoder, after the
 - 7 non-compliant data is replaced with compliant data.
- 1 2. The method as recited in claim 1, further comprising:
 - 2 encrypting a portion of the data stream; and
 - 3 transmitting the portion of the data stream.
- 1 3. The method as recited in claim 2, further comprising:
 - 2 decrypting the portion of the data stream.
- 1 4. The method as recited in claim 3, wherein the non-compliant data is key
2 information that is used in encrypting and decrypting.
- 1 5. A method, comprising:
 - 2 receiving a portion of a data stream;
 - 3 parsing the portion of the data stream to find a synchronization point
 - 4 within the data stream;
 - 5 retrieving non-compliant data near the synchronization point; and
 - 6 decrypting the portion of the data stream.
- 1 6. The method as recited in claim 5, wherein the non-compliant data is key
2 information that is used in decrypting.
- 1 7. The method as recited in claim 5, further comprising:
 - 2 replacing the non-compliant data near the synchronization point with

3 compliant data; and
4 decoding the portion of the data stream.

1 8. A system, comprising:
2 an authoring device to use key information to encrypt a portion of a data
3 stream; and
4 a consumption device in communication with the authoring device, the
5 consumption device to use the key information to decrypt the portion of the data
6 stream.

1 9. The system as recited in claim 8, further comprising:
2 a decoding device in communication with the consumption device to
3 decode the portion of the data stream.

1 10. The system as recited in claim 8, wherein the consumption device is
2 configured to retrieve the key information from the portion of the data stream.

1 11. A system, comprising:
2 an authoring device to create a data stream;
3 an encryption tool to embed key information near each synchronization
4 point in the data stream and to encrypt a portion of the data stream associated
5 with each synchronization point; and
6 a consumption device to retrieve key information near each
7 synchronization point in the data stream and to replace the key information with
8 compliant data and to use the key information to decrypt the data stream.

1 12. The system as recited in claim 11, further comprising:
2 a decoding device to decode the data stream.

1 13. The system as recited in claim 11, further comprising:
2 a decryption tool to use the key information to decrypt the portion.

1 14. A machine-accessible medium having associated content capable of
2 directing the machine to perform a method, the method comprising:
3 parsing a first data stream to find a packetized elementary stream (PES)
4 header, the PES header associated with at least some payload data;
5 copying the first data stream to a second data stream; and
6 selectively inserting compliant data into the second data stream after the
7 PES header, to hold key information associated with the PES header.

1 15. The machine-accessible medium as recited in claim 14, wherein the
2 method further comprises:
3 storing the first data stream; and
4 storing the second data stream.

1 16. The machine-accessible medium as recited in claim 14, wherein the
2 method further comprises:
3 parsing the second data stream to find each PES header;
4 embedding key information into each portion of the second data stream
5 after each PES header; and
6 encrypting each portion of the second data stream.

1 17. The machine-accessible medium as recited in claim 16, wherein the
2 method further comprises:
3 transmitting each portion of the second data stream.

1 18. The machine-accessible medium as recited in claim 16, wherein the
2 method further comprises:
3 retrieving key information from a portion of the second data stream;
4 decrypting the portion of the second data stream with the key
5 information; and
6 replacing the key information with compliant data in the portion of the
7 second data stream.

1 19. The machine-accessible medium as recited in claim 18, wherein the
2 method further comprises:
3 decoding the portion.

1 20. A data structure, comprising:
2 a header;
3 key information associated with the header for use in decryption; and
4 a payload associated with the header, the payload capable of being
5 encrypted using the key information.

1 21. The data structure as recited in claim 20, wherein compliant data replaces
2 the key information associated with the header, before decryption.

1 22. The data structure as recited in claim 21, wherein the header, compliant
2 data, and decrypted payload are capable of being decoded by a compliant
3 decoder.

1 23. The data structure as recited in claim 20, wherein the key information in
2 the header replaces compliant data, after encryption.

1 24. The data structure as recited in claim 20, wherein the header is a
2 packetized elementary stream (PES) header and the payload is a PES payload.

1 25. A data stream stored on a machine-readable medium, the data stream
2 comprising at least one data structure as recited in claim 20.